C/CSG/05

DIRECTOR OF CENTRAL INTELLIGENCE
Intelligence Information Handling Committee
WASHINGTON, DC 20505

ICS - IHC/MM 86-19
31 MAR 1986

25X1 MEMORANDUM FOR: [redacted]
Deputy Director of NSA for Information Security

SUBJECT: Request for R&D and Operational Support from the National Computer Security Center

REFERENCE: NSA Ltr dtd 26 Feb 86, Subject: FY88-92 National Automated Information System Security (AISS) Program Guidance.

1. Per reference, we appreciate the opportunity to identify R&D and operational requirements for automated systems and networks processing information within the Intelligence Community (IC). Our response has been delayed so that it could be coordinated with the members of the committee at our 28 March Information Handling Committee (IHC) meeting. There was agreement among the members of the IHC that the identified efforts will improve current shortfalls in a significant number of IC automated systems and networks. I offer the IHC as a mechanism for working with Intelligence Community components in support of our mutual efforts to protect information
25X1 processed in automated systems. [redacted]

25X1 [redacted]

3. The resources identified within the NFIP are also being used to implement non-technical security SAFEGUARDS such as the expansion of staff personnel who will maintain the access control facilities and review the audit materials being produced as a result of upgrading the security features of IC systems. The IC is also acquiring security-enhanced components such as access control devices, analyst workstations, and automated support tools to assist

25X1 [redacted]

25X1 SECRET [redacted]

security officers in the review of audit trail material. In addition, we are also reviewing the current use of security labels within automated information systems and networks in the Community to determine what modifications in practices and procedures may be necessary in order to use the "trusted" products being identified by the NCSC.

25X1

4. Attachment 1 summarizes our request for R&D and operational support from the NCSC. The remaining attachments identify our requirements and resource estimates in the format you requested. We appreciate your efforts in support of our requirements.

25X1

Chairman

Attachments:
As stated

Attachment 1

FOR OFFICIAL USE ONLY

REQUEST FOR R&D AND OPERATIONAL SUPPORT FROM

NATIONAL COMPUTER SECURITY CENTER

- 0 BLACKER - Completion of current Phase I development and fielding
- 0 IS/A-AMPE - Continued support thru full implementation
- 0 DoDIIS Network - Continued support thru full implementation
- 0 Expansion of EPL - Evaluate "trust" of current & new product lines commonly used in the IC (e.g., DEC, WANG, UNIVAC, CRAY)
- 0 Component Products List - Develop a NCSC "certified" Products List for COMPONENT products to be used with "trusted" systems (e.g., biometric devices, PCs/WS, LANs, call-back devices)
- 0 Call-back Devices - Provide an evaluated list of "trustworthy" automatic call-back devices for use with dial-up systems. Identify other acceptable devices that can be procured in the near term to reduce risks.

FOR OFFICIAL USE ONLY

FOR OFFICIAL USE ONLY

REQUEST FOR R&D AND OPERATIONAL SUPPORT FROM

NATIONAL COMPUTER SECURITY CENTER

(Continued)

- Orange Book Guidelines - Provide guidelines for the use of "orange book" criteria in performing technical evaluations of hardware/software (e.g., covert channel analysis, trusted path, verified design)

- Technical H/S Evaluation Support - Upon request, provide hardware/software technical evaluation support to certify baseline hardware and software in support of IC formal accreditation processes

- Biometric Device Integration - In conjunction with DIA, develop and certify software and procedures for integrating the use of biometric access control devices into selected automated systems used by the IC (e.g., SUN and IBM PCs, sensitive systems)

- Controlled Release of Trusted Systems - Perform research to determine way(s) that technical modifications might be made to some class(es) of "trusted systems" for export/sale to foreign customers without compromising US systems

FOR OFFICIAL USE ONLY

REQUEST FOR R&D AND OPERATIONAL SUPPORT FROM

NATIONAL COMPUTER SECURITY CENTER

(Continued)

- PC/WS Storage Encryption - In coordination with the Commercial COMSEC Endorsement Program (CCEP), develop and certify methods and procedures for using encryption devices to encrypt data on floppy disks, hard disks and possibly data in communications buffers. Priority on SUN and IBM.

- Floppy Disk Detection Capability - Determine the feasibility of developing a floppy disk detection capability to avoid inadvertent/intentional removal from sensitive facilities. Possibly like detection devices used in airports.

- Secure DBMS - Develop guidelines and work with specified DBMS vendors who support the IC to implement appropriate security in DBMS(s) so that they will provide compatibility with "trusted systems". Priority for the IC is Model-204.

Next 2 Page(s) In Document Denied

National Computer Security Program
Automated Information Security
Research and Development
FY-88-92

Problem: Security features/characteristics of major system hardware/software need to be evaluated and "certified" before procurement

Requirement: Need for identification of "trusted" products that can be procured by the Intelligence Community

Recommended Program: Expansion of the EPL - Evaluate "trust" of current & new product lines commonly used in the IC (e.g., DEC, WANG, UNIVAC, CRAY)

25X1

Submitted by: [redacted] ICS/IHC [redacted]
(Include POC and phone number)

Organization to Perform: National Computer Security Center

Estimated Funding: (Thousands of Dollars)

FY-87	FY-88	FY-89	FY-90	FY-91	FY-92
As identified in the NCSC program and budget					

Attachment 6

National Computer Security Program
Automated Information Security
Research and Development
FY-88-92

Problem: Security of "component" products needs to be evaluated and "certified" before procurement

25X1

Requirement: Need for identification of "component" products that can be procured by the IC

Recommended Program: "Component" Products List - Develop a NCSC "certified" Products List for COMPONENT products to be used with "trusted" systems (e.g., biometric devices, PCs/WS, LANs, call-back devices)

25X1

Submitted by: [redacted] ICS/IHC [redacted]
(Include POC and phone number)

Organization to Perform: National Computer Security Center

Estimated Funding: (Thousands of Dollars)

FY-87	FY-88	FY-89	FY-90	FY-91	FY-92
25X1					

CONFIDENTIAL

Attachment 8

National Computer Security Program
Automated Information Security
Research and Development
FY-88-92

Problem: Need clarification on how to use the "Orange Book" for technical security evaluations in support of the formal accreditation process.

Requirement: Provide guidelines for the use of "orange book" criteria in performing technical evaluations of hardware/software (e.g., covert channel analysis, trusted path, verified design)

Recommended Program: Orange Book Guidelines

25X1

Submitted by: [redacted] ICS/IHC [redacted]
(Include POC and phone number)

Organization to Perform: National Computer Security Center

Estimated Funding: (Thousands of Dollars)

FY-87	FY-88	FY-89	FY-90	FY-91	FY-92
$100	$100	75	--	--	--

CONFIDENTIAL

Next 5 Page(s) In Document Denied